Capabilities for Strengthening Cybersecurity Resilience

In the Homeland Security Enterprise

September 2012

Homeland Security

DHS Cybersecurity Strategy

- A cyberspace that:
  - Is Secure and Resilient
  - Enables Innovation
  - Protects Public
  - Advances Economic Interests and National Security
- Resilience
  - Fostering individual, community, and system robustness, adaptability, and capacity for rapid response and recovery
  - Be prepared to maintain critical operations in a degraded environment

Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise

Focus Area: Strengthening the Cyber Ecosystem

Homeland Security

What is the *Cyber Ecosystem*?

- **The cyber ecosystem is global, evolving and includes government and private sector information infrastructure; the interacting persons, processes, data, information and communications technologies; and the environment and conditions that influence their cybersecurity**

Homeland Security

DHS Cyber Ecosystem White Paper

- The paper explores the idea of a future cyberspace that is:
  - Healthy
  - Resilient
  - Fundamentally more secure
- Resilience
  - Improve the reliability and resilience of critical infrastructures
  - Sustain agreed-upon service levels
  - Automated configuration adjustments in response to trust choices would offer increased reliability and resilience

Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action

Homeland Security

Physical and Cyber Resiliency Components of the Cyber Ecosystem

- Physical
  - Supporting Infrastructure (i.e., power, water, etc)
  - Communications
  - Hardware
  - Software
  - Human organizational
  - Data
- Cybersecurity
  - Supporting Infrastructure (i.e., power, water, etc)
  - Communications
  - Hardware
  - Software
  - Human organizational
  - Data confidentiality integrity, and availability

Homeland Security

Strengthening the Cyber Ecosystem

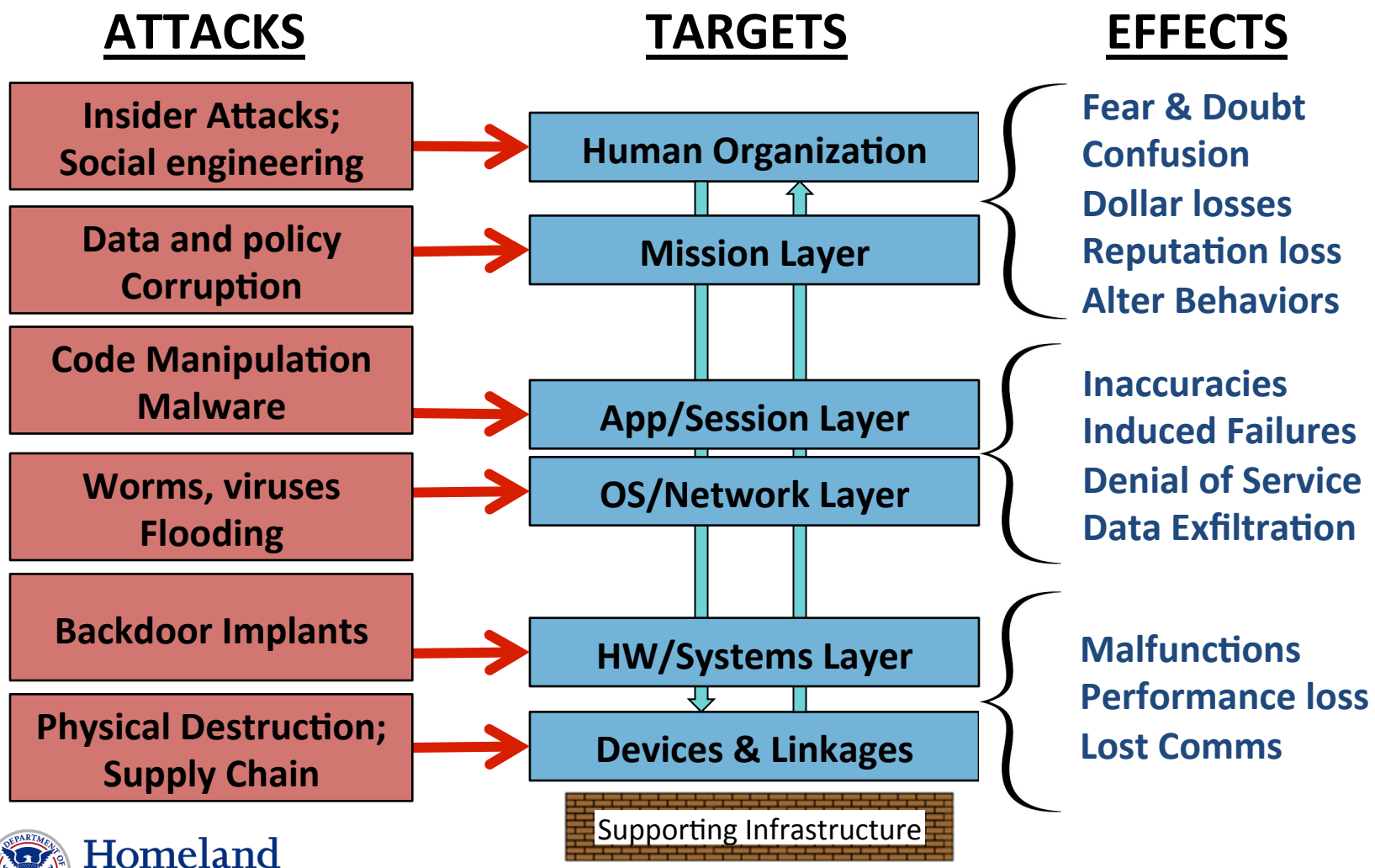
- **Today**
  - Many unknown vulnerabilities
  - Incidents propagate at machine speeds and Defenses are manual
  - Many intrusions are undetected
  - Each system is defended independently
  - Inconsistent security policies
  - Users don't follow best practices
  - Attacks increasing in number and virulence

- **Future**
  - Security is built-in, reducing vulnerabilities
  - Many attacks but less impact
  - Unauthorized activity more quickly identified
  - Automated defenses used appropriately
  - Information sharing; collaborative defense used when appropriate
  - Consistent security practices
  - Near-real-time responses
  - Ability to learn and adapt defenses in near-real time

Adversaries will continue to have robust and evolving capabilities

Homeland Security

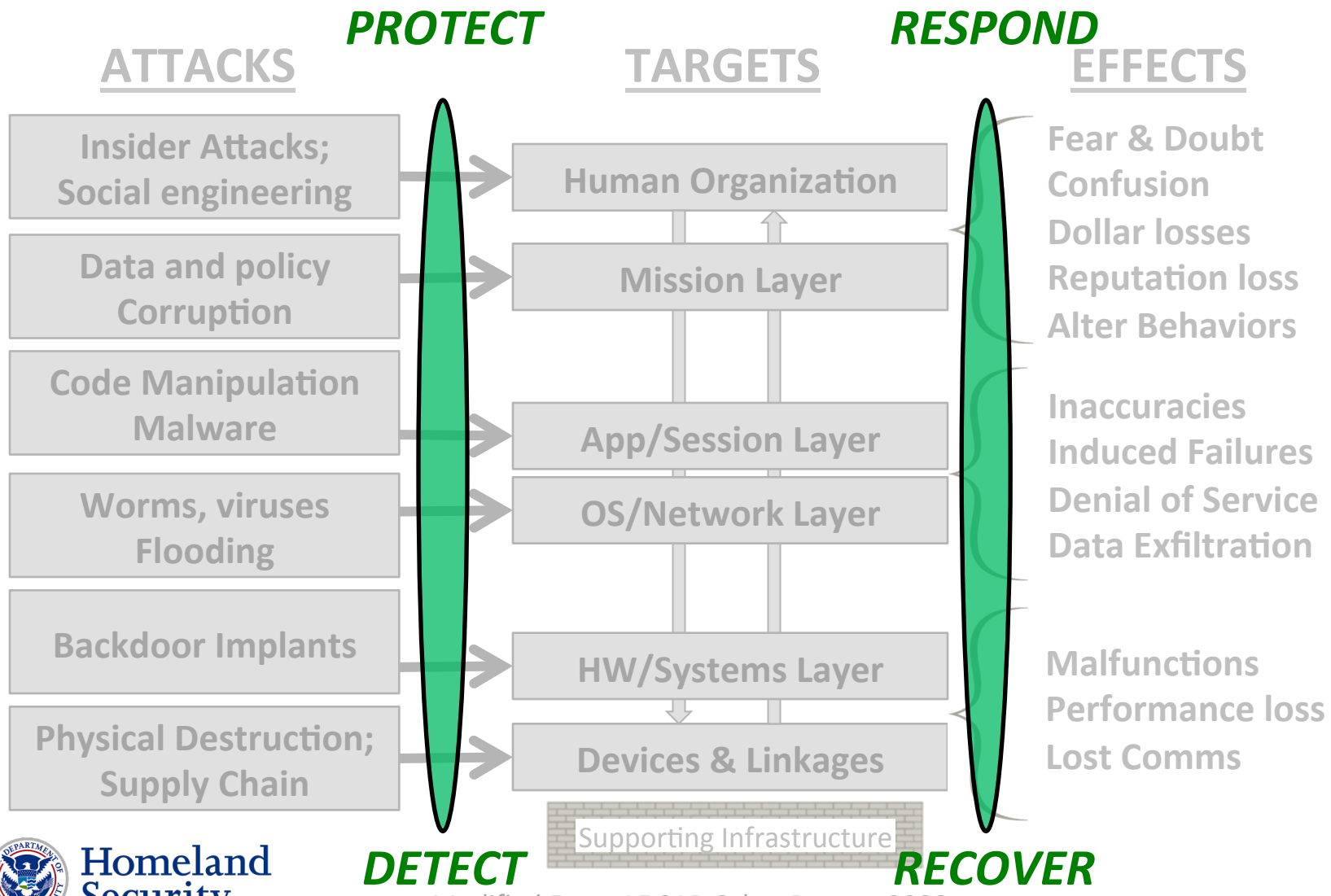
Cyber Attacks, Targets, Effects



Homeland Security

Modified From AF SAB Cyber Report, 2008

Cyber Attacks, Targets, Effects



Homeland Security

Modified From AF SAB Cyber Report, 2008

Desired Capabilities - Protect

- Security is built in
- Increased information sharing and collaboration, vertically and horizontally
- Risk based data management
- Automated collective protection *when appropriate*
- Tailored trustworthy spaces
- Moving target
- Authentication appropriate to use case
- Increased user awareness and education

Protect while Ensuring Privacy

Homeland Security

Desired Capabilities - Detect

- Information sharing & collaboration, vertically and horizontally
- Continuous monitoring
- Authentication
- Built in security
- Awareness and Education
- Business rules based Behavior monitoring
- Situational Awareness

Detect while Ensuring Privacy

Homeland Security

Desired Capabilities - Respond

- Increased information sharing, vertically + horizontally
- Automated collective response *when appropriate*
- Moving Target
- Authentication
- Machine learning and evolution
- Assessment, forensics, and remediation
- Feedback and Lessons Learned

Respond while Ensuring Privacy

Homeland Security

Desired Capabilities - Recover

- Situation awareness, information sharing and collaboration
- Machine learning and evolution
- Interoperability
- Automated recovery
- Authentication

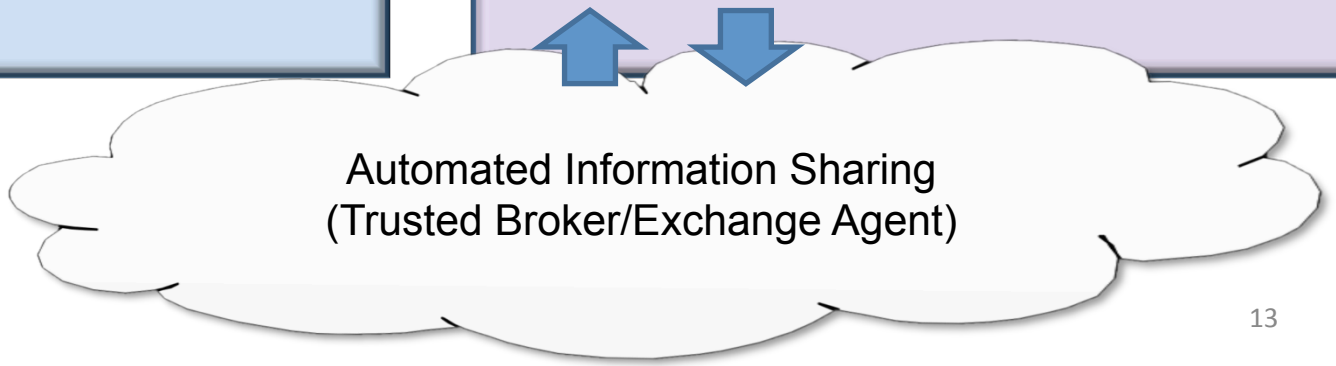
Recover while Ensuring Privacy

Homeland Security

Improving Cybersecurity via Automated Collective Action

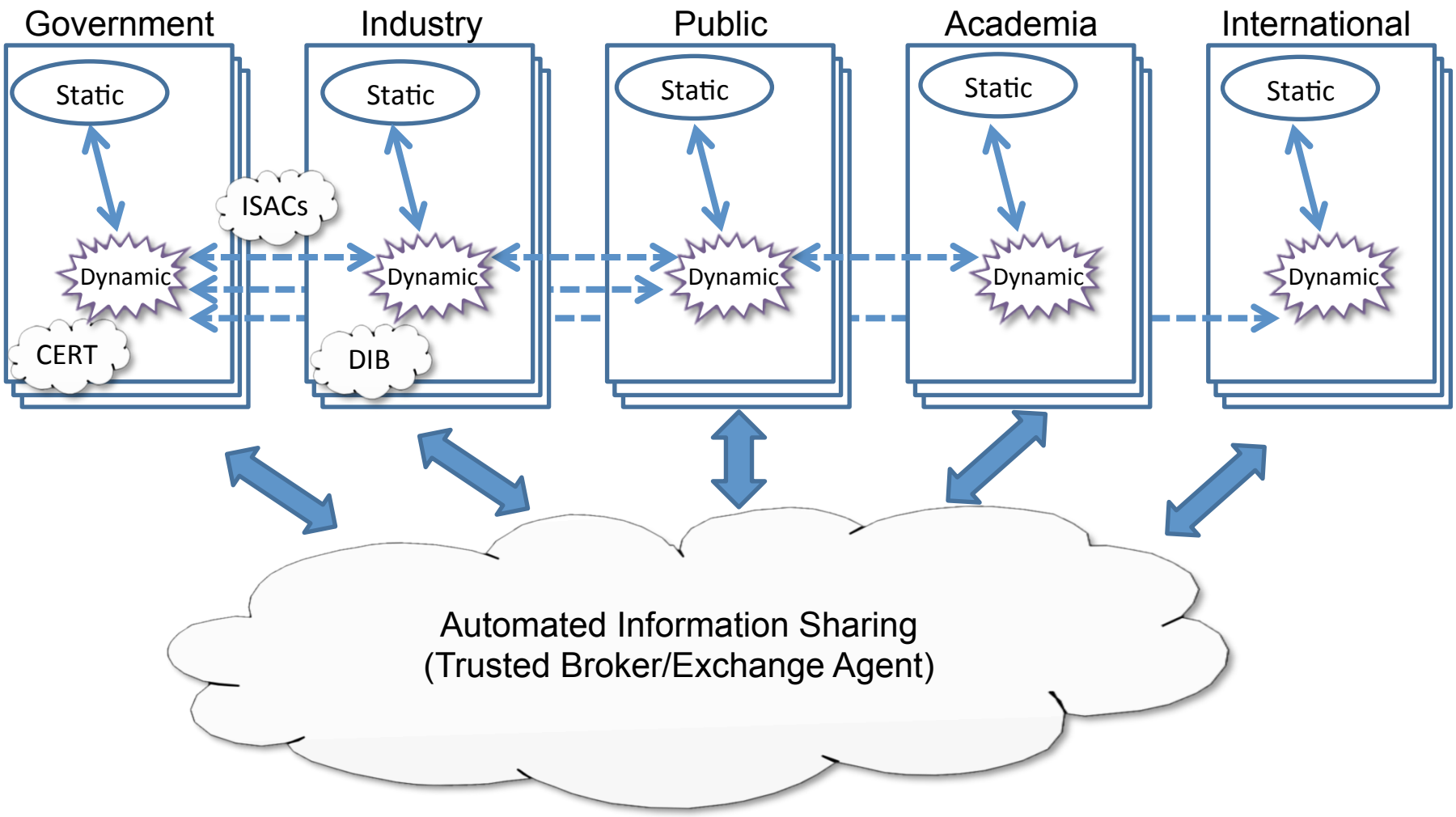
- Static Defense (put the infrastructure in the best possible condition – hygiene)
  - Prevent
    - Continuous Authentication, Authorization
    - General Awareness and Education
    - Interoperability
    - Machine Learning and Evolution
    - Moving Target
    - Privacy
    - Risk-Based Data Management
    - Security Built in
    - Situational Awareness
    - Tailored Trustworthy Spaces
  - Detect
    - Continuous monitoring
    - Behavior monitoring based on business rules
    - Sensors

- Dynamic Defense (respond to situation)
  - Real time Information sharing
    - Continuous information sharing and exchange with cloud
    - Situational Awareness
    - Analysis
  - Respond
    - Automated Identification, Selection, and Assessment of Defensive Actions
    - Adjustments, automated courses of action
    - Share courses of action
  - Recover
    - Automated courses of action
    - Manual cleaning, patching, and configuration



Homeland Security

Automated Collective Action throughout the Ecosystem



Homeland Security

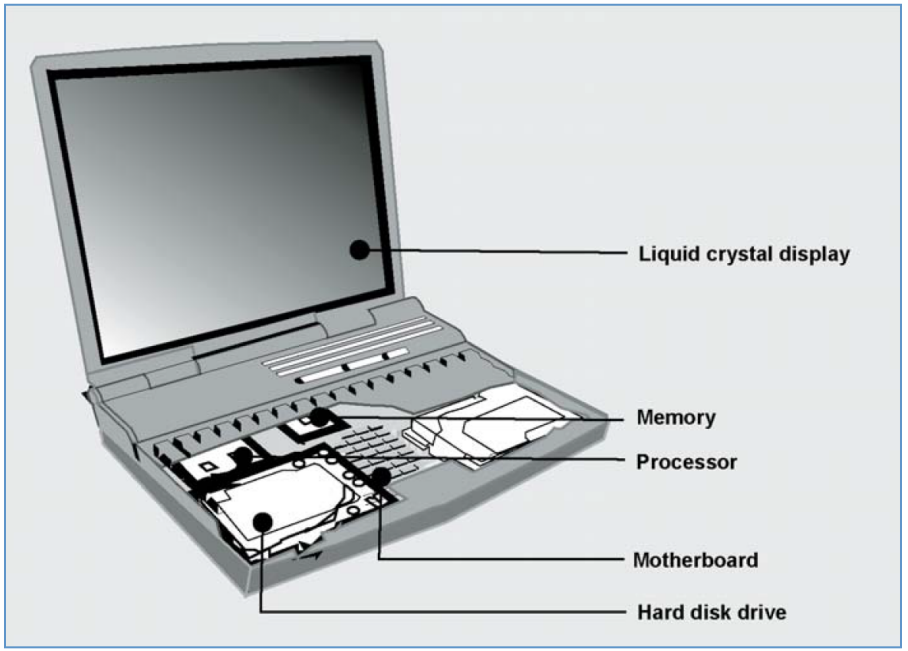
Resiliency Must Address these Trends

- Supply Chain Vulnerabilities
- Cloud Computing
- Mobile technologies
- Bring Your Own Devices (BYOD)
- Others…

Homeland Security

Common Suppliers of Laptop Components

- Liquid Crystal Display
  - China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
- Memory
  - China, Israel, Italy, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, United States
- Processor
  - Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
- Motherboard
  - Taiwan
- Hard Disk Drive
  - China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States



Homeland Security

Source: GAO Report GAO-12-361

Threats to the IT Supply Chain

- Installation of hardware or software containing malicious logic
- Installation of counterfeit hardware or software
- Failure or disruption in the production or distribution of critical products
- Reliance on a malicious or unqualified service provider for the performance of technical services
- Installation of hardware or software that contains unintentional vulnerabilities

Source: GAO Report GAO-12-361

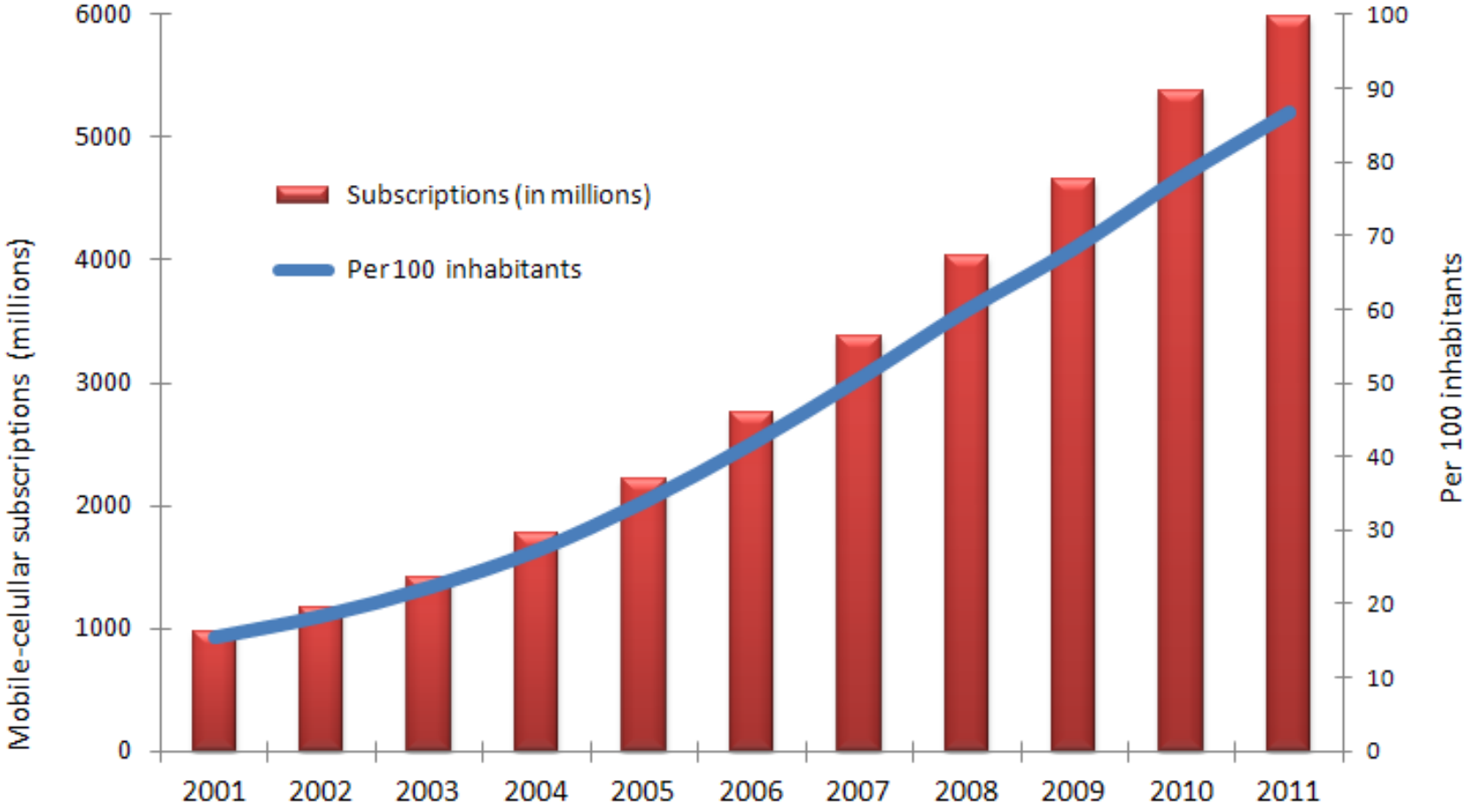
Cloud Computing Trends

- Gartner projects cloud computing to grow 20 percent annually
  - Some estimate 30 percent annually for the next few years
- Global market for cloud computing services is expected to reach $42 billion by end of 2012
  - Gartner estimates growth to be $150 billion in 2013

Homeland Security

Sources: FCW and Federal News Radio

Growth in Mobile Phone Subscriptions

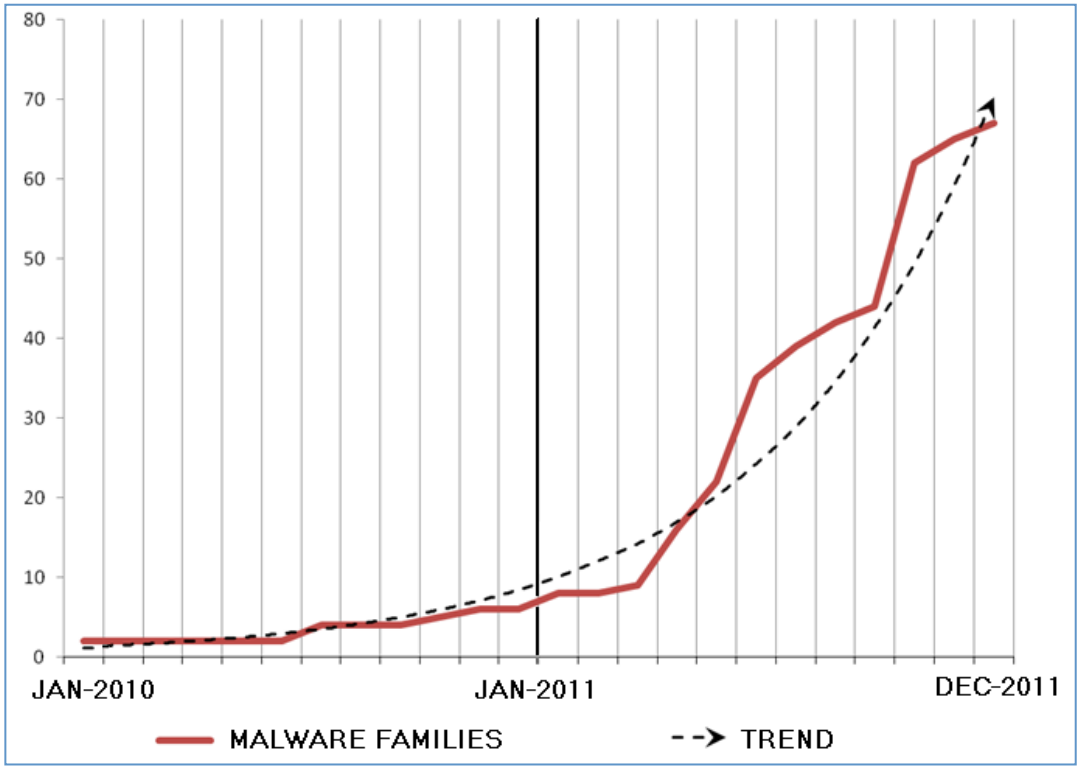


Homeland Security

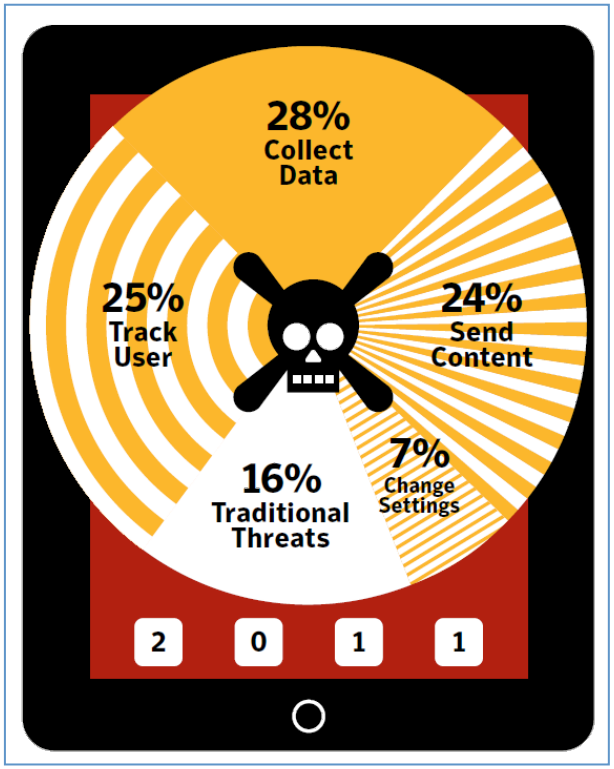
Source: ITU World Telecommunications/ICT Indicators database

Malware on Your Mobile Phone

Number of Mobile Malware Families



Mobile Malware Functionality



Homeland Security

Source: Symantec

Bring Your Own Device

- "BYOD"
  - Employees bring their own portable computing devices to the workplace for use, often with connectivity to the corporate network
  - Smart phones, Laptops, Tablets, PDAs
- Users have purchased better technology than their employer can afford to provide
  - Prohibiting BYOD is not necessarily the answer
  - Allowing, but not managing, BYOD is irresponsible

Making BYOD Work

- Employers:
  - Create Policy & Guidance for Acceptable BYOD Use
    - Educate Employees
    - Know when to Say "No"
    - Use Applications to Lock/ Wipe/Locate Devices
    - Secure Messages
  - Control Access
  - Staff up to Support BYOD
- Employers (continued)
  - Support Multiple Platforms
    - Track Applications and Devices
    - Control patches & updates
  - Use Security Framework
- Industry:
  - Develop
    - Standards
    - Security frameworks
    - Secure operational environments

Homeland Security

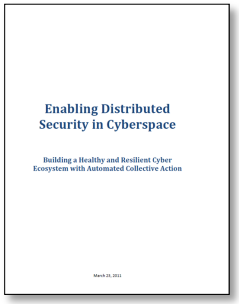
Source: GCN

Next Steps

- Continue to Evolve Required Cyber Ecosystem Capabilities
  - Cyber Ecosystem RFI to be jointly issued by DHS and NIST
  - Continue efforts with NSA
- Incorporate requirements into planning/budget process
- Continue near term automation and information sharing efforts
  - Trusted Automated Exchange of Indicator Information (TAXII)
  - DHS CRADAs
- Work with R&D communities on cyber requirements

Cyber Ecosystem RFI

- DHS and NIST jointly published Cyber Ecosystem Request for Information
  - Learn more about concept of using automated collective action between information systems and cyber devices to strengthen cybersecurity
  - Learn about related research and technologies from industry and academia
  - Identify unintended consequences of automated collaborative action
- A stronger cyber ecosystem combines local & global alerting and response
  - Inform other ecosystem participants of attack, before coming under attack
  - Help defend against the attack before it spreads
- To download the Cyber Ecosystem RFI:
  - On **www.fbo.gov**, search for Solicitation **RFI-OPO-12-0002**
  - RFI responses requested by October 1
- To download the DHS Cyber Ecosystem white paper:
  - **www.dhs.gov/enabling-distributed-security-cyberspace**



Homeland Security

Summary

- Future Cyber Ecosystem
  - Proactive, not reactive, cyber defenses
  - Automated Collective Action when appropriate
  - Improved resiliency
- Desired Cybersecurity Capabilities
- Trends Impacting Cyber Ecosystem
  - Very likely to exacerbate security challenges

Backups

Desired Cyber Ecosystem Capabilities

- Automated Identification, Selection, and Assessment of Defensive Actions
- Authentication
- Business Rules-Based Behavior Monitoring
- General Awareness and Education
- Interoperability
- Machine Learning and Evolution
- Moving Target
- Privacy
- Risk-Based Data Management
- Security Built in
- Situational Awareness
- Tailored Trustworthy Spaces

Define the Layers

- **Human and Organization**: The mission is executed at this layer.
- **Mission**: Includes mission capabilities such as command and control or weapon systems.
- **Application and Session**: Includes applications such as databases and web browsers.
- **Operating System and Network**: Protocols and components such as routers and firewalls, along with their associated operating software.
- **Hardware and Systems**: Central processing units (CPUs) and storage arrays.
- **Devices and Linkages**: Materials and devices that provide the underpinnings of computing devices and networks. This layer includes communication links and electronic devices such as wires, antennas, transistors, and chips.

Automated Collective Action

- The processes in a cyber ecosystem or community of interest (COI) that **select (and perhaps formulate) automated courses of action that will be performed by the ecosystem or COI in response to cybersecurity events**.
  - Policies, procedures, technology, and a high level of trust are necessary to enable automated collective action.
  - An appropriate level of human intervention might be required to ensure unintended consequences don't result from flawed courses of action.
  - Determining which cybersecurity events are normal and which are unauthorized or malicious remains a major challenge.
- Cyber equivalent of the human immune system.

Capability Maturity at Each Layer

	Auto-mation; Select ACOAs	Authen-tication	Inter-oper-ability	Machine Learning and Evolu-tion	Build Security In	Rules-Based Behavior Monitoring	Aware-ness & Educa-tion	Moving Target	Privacy	Risk-Based Data Mgmt	Situa-tional Aware-ness	Tailored Trust-worthy Spaces
Human												
Mission												
Session												
OS/Net												
H/W												
Physical												

⇦ More Capability Less Capability ⇨

Homeland Security

Note: Maturity Levels are Subjective

A Future Ecosystem Incorporates Multiple Capabilities within the three Functional Areas of Technology, Process, and People

Technology

- Healthy cyber devices will incorporate standards-based authentication, interoperability, automation
- Business rules based malicious behavior detection, and risk based data management
- Cyber devices will provide security, affordability, ease of use and administration, scalability, and interoperability
- Barriers to automated collaboration are based on policy, not technology limitations

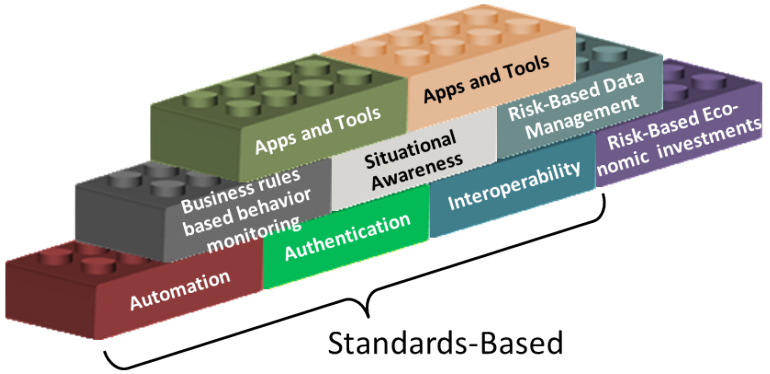
Process

- Incentives for information sharing
- Organize cyber defense so that machines defend against machines and people defend against people
- Economic based decision process – risk based cybersecurity investments

People

- The healthy cyber participants have continuing access to a range of education, training, and awareness opportunities
  - Such as exercises, simulations, and fully-immersive learning environments
- Have validated skills that have been codified for their occupations or positions and strongly proofed cyber identities

Foundations of the Cyber Ecosystem



Attributes of the Cyber Ecosystem

An integrated security operating foundation that is:

- Cost effective
- Flexible
- Interoperable
- Stable
- Enables rapid integration of new capabilities from multiple sources
- Moving target

Homeland Security